Before the Federal Communications Commission
Washington, D.C. 20554

In the Matter of Framework for Next Generation 911 Deployment
PS Docket No. 10-255

Reply Comments of the Privacy Rights Clearinghouse

March 14, 2011

The Privacy Rights Clearinghouse (PRC) respectfully submits the following comments to the Federal Communications Commission for its consideration with respect to the Notice of Inquiry *in the Matter of the Framework for Next Generation 911 Deployment*, PS Document No. 10-255.[1]

I. Background

The PRC is a nonprofit organization, established in 1992 and located in San Diego, California. Our mission is two-part: consumer education and consumer advocacy. We have published more than 50 Fact Sheets that provide practical information covering strategies that consumers may employ to safeguard their personal information.

The PRC also invites individuals to contact the organization with their questions, concerns and complaints. Over the course of our 19-year history, PRC staff members have worked directly with tens of thousands of consumers. Our positions reflected in the comments below reflect, in large part, our observations based on direct communication with individual consumers over the years.

II. General Statements

The Federal Communications Commission's initiative to transition from the legacy 911 system to a broadband Internet Protocol (IP)-based system capable of supporting multimedia is a commendable effort to improve 911 response and public safety. As it moves forward with Next Generation 911 (NG911), we urge the Commission to continue to systematically analyze and address potential consumer privacy concerns. It is especially important that the Commission work to safeguard sensitive medical and location-based data.

Consumers have high expectations when it comes to the privacy of data they consider sensitive. Actual or perceived loss of expected privacy would likely have a chilling effect on consumer use

[1] FCC, *Framework for Next Generation 911 Deployment*, Notice of Inquiry, PS Docket No. 10-255 (rel. Dec. 21, 2010) para. 76 [hereinafter NOI], *available at* http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db1221/FCC-10-200A1.pdf (published in the Federal Register on Jan. 13, 2011).

of 911 systems during emergency situations, thus underutilizing NG911's intended benefits. To retain consumer trust and avoid undermining NG911 system capabilities, all entities handling data associated with 911 calls, namely Public Safety Answering Points (PSAPS), must be subject to robust, relevant, and effectively enforced privacy regulations. Furthermore, individuals must retain maximum control over personal data, and be afforded adequate educational opportunities so they remain informed of NG911 benefits and capabilities.

III. Responses to Specific Inquiries

Primary vs. Secondary Usage of Media Types

Paragraph #39: In some cases, primary media may not be available to a 911 caller (e.g. due to network congestion or end system limitations). In these cases, we seek comment on whether e-mail or social network status pages could possibly be used as the primary means of contacting a PSAP?

The NOI suggests that social network status pages would be used as a primary means of communication with PSAPs on a very limited basis. We encourage the Commission to follow through with this approach. It is true that there will likely be emergency situations in which using social media to communicate an emergency will benefit a consumer. However, monitoring social media for any reason, including public safety, should be limited to the most extreme circumstances under which other modes of communication would be impractical or completely unavailable.

As such, we urge the Commission to consider (on a case-by-case basis when practicable) laying out a process under which privacy risks must be fully discussed, addressed, and implemented in a comprehensive Fair Information Practices (FIPs)-based plan.[2] Any such plan must seek to minimize sensitive data collection, retention, and sharing.

Paragraph #40: Should different standards or requirements apply to primary conversational media as opposed to secondary non-conversational media? If secondary non-conversational media include the capability to transmit sensitive personal data, what privacy protection concerns are raised and how should they be addressed?

As the Commission is aware, 911 calls are public record in most states.[3] If communications using primary media (listed as voice, RTT, and SMS)[4] are considered analogous to the current system's calls and remain largely public record, it will be imperative to differentiate between

[2] For an in-depth analysis of the issue of social media monitoring, we point the Commission to the Electronic Frontier Foundation's (EFF) work surrounding its Freedom of Information Act requests regarding social media monitoring. *See* Jennifer Lynch, *New FOIA Documents Reveal DHS Social Media Monitoring During Obama Inauguration*, EFF DEEPLINKS BLOG, Oct. 13, 2010, http://www.eff.org/deeplinks/2010/10/new-foia-documents-reveal-dhs-social-media/ (last visited March 8, 2011).

[3] *See e.g. States eye ban on public release of 911 calls*, ASSOC. PRESS, Feb. 23, 2010, *available at* http://www.msnbc.msn.com/id/35547155/ns/us_news-life/. (last visited March 11, 2010).

[4] "RTT" refers to Real Time Text and "SMS" refers to Short Message Service.

primary and secondary media (media that may convey additional information) to better protect personal data. Neither sensitive data nor records should be accessible to the public merely because they are associated with a 911 call.

Applying privacy protection standards across the board to information transmitted in addition to the "call" would help instill consumer confidence in NG911 systems from the point of implementation. For example, victims of stalking and domestic violence must take great measures to protect their privacy on all fronts and may fear making a call to a 911 system that they do not trust will protect their personal information. Because consumer opinions differ as to what constitutes "sensitive" information, we encourage the Commission to enact strong protections encompassing all secondary media transmissions, with special attention paid to medical and location data.

The Commission should also note that consumers may be unaware of the information they are sharing with PSAPs when they use additional forms of media to contact emergency services. For example, smart phones and modern cameras may transmit information via metadata (such as the type of device used, the time, the exact location, etc.), which would then become part of the call record if the consumer transmits a photo to a PSAP. We urge the Commission to treat metadata as nonpublic information.

Furthermore, we advise the Commission to investigate whether the transition to NG911 should also be a transition to a nonpublic call record system, as future "call records" may contain a wealth of knowledge beyond the traditional emergency services phone call.

SMS for Emergency Communications

Paragraph #47: Transmitting Medical Data

Should medical information be provided in the ordinary course to EMS and other first responders in a manner similar to the provision of medical condition information described in paragraph #37? Since privacy protection concerns would seemingly be implicated in this case, as in the case of transmitted medical information, how should such concerns be addressed?

The ability to place a 911 call and transmit medical information simultaneously to first responders has the potential to enhance emergency response effectiveness, but presents challenges regarding consumer privacy protection. As PSAPs become capable of receiving, storing, and/or transmitting electronic medical data, they must be required to observe relevant privacy laws. At a minimum, PSAPs must be held accountable under existing state and federal privacy laws, and we suggest that the Commission further analyze the relevant laws to determine their application and sufficiency.[5]

[5] *See* Public Safety Communications, *HIPAA Didn't Kill the Radio Star*, Aug. 26, 2010, http://psc.apcointl.org/2010/08/26/hipaa-radio-emd/ (last visited March 11, 2011); Douglas Wolfberg, Stephen Wirth, & Cindy Staffelbach, *HIPAA: The Intersection of Patient Privacy with Emergency Dispatch,* http://www.911dispatch.com/info/hipaa_position.pdf (last visited March 11, 2011) (both suggesting that it is unclear to what extent current dispatch centers are affected by HIPAA).

Consumers must have reason to trust that their medical records and data are handled with appropriate care. We suggest that the Commission also consider the importance of minimizing data retention practices and develop a uniform process to handle data breaches and notify all affected individuals.

Furthermore, consumers deserve to retain maximum control over their medical records, especially in determining when and whether they authorize PSAPs to forward their data. If possible, we advocate allowing the caller to decide whether and/or what to transmit at the point where the call is made. Individuals must also be able to access their information to change or delete it. This is especially true if information is provided to a PSAP on a prior-consent basis (as is a noted possibility in NOI paragraph #38) to be forwarded to first responders.

Confidentiality and Privacy Concerns

Paragraph #75: What privacy concerns will be introduced with the deployment of NG911?

The PRC applauds the Commission's concern regarding consumer privacy. Baking consumer privacy protections into an NG911 system will allay many of these concerns. Ideally, PSAPs will be held accountable by way of a comprehensive privacy policy. We recommend any governing policy be based on the full set of FIPs and be completely enforceable. PSAPs must also be subject to robust data breach notification policies. Our primary concerns include the transmission and handling of medical data (addressed above) and location data, but also extend to further NG911 capabilities set forth in the NOI.

As PSAPs become equipped to handle an influx of multiple forms of consumer information, the potential for employees to jeopardize consumer privacy by disclosing and/or selling any non-public information must be fully addressed. For example, hospital employees have been known to sell celebrity medical data to tabloids for personal gain,[6] and nurses at a San Diego county hospital were recently fired for posting patient information on social media pages.[7] Hospital employees have even sold non-celebrity data for a profit.[8]

To minimize the potential for abuse, PSAP staff must receive extensive and ongoing training and be subject to rigorous monitoring and strict enforcement if such abuses are discovered.

Location information[9]

[6] *See* Charles Ornstein, *Fawcett's cancer file breached*, LA TIMES, Apr. 3, 2008, http://articles.latimes.com/2008/apr/03/local/me-farrah3 (last visited March 14, 2011).

[7] *See* Michael Burge, *5 fired for discussing patients' cases online*, SAN DIEGO UNION TRIB., June 10, 2010, http://www.signonsandiego.com/news/2010/jun/10/5-employees-fired-for-discussing-patients-cases/ (last visited March 14, 2011).

[8] See Privacy Rights Clearinghouse's Chronology of Data Breaches: Security Breaches 2005-Present, http://www.privacyrights.org/data-breach (last visited March 14, 2011) for multiple examples.

[9] *See* NOI, supra note 1, para 76.

Many consumers consider their location information to be highly sensitive. As the Commission moves forward with its plan to bring the 911 system up-to-date with current technology, it must consider how to best protect this information from being misused. If the system relies on service providers to determine location information, it must also take into account the fact that such information is increasingly valuable. Because of this value and the potential for abuse by third parties, we encourage the Commission to develop measures to ensure that entities outside of the 911 system are unable to sell and/or use this data for unrelated purposes.

Device-Initiated Services for Emergency Communication[10]

In an IP-based network architecture, emergency calls can be placed not only by human beings, but by a variety of automatically triggered devices. Examples of the devices include security cameras, alarms, personal medical devices, telematics, and consumer electronics in cars.

The PRC is concerned that the NOI's section discussing device-initiated services for emergency communications does not address consumer choice. Notwithstanding any benefit that consumers may incur because a device can automatically contact 911, the choice of whether and when to enable these devices should rest wholly with the individual consumer. This choice could be in the form of a persistent authorization for the device to contact 911 under certain circumstances, or, preferably, could be presented each time a triggering incident occurs.

Consumers must also be able to access information about their selected preferences and edit them if they so desire. To illustrate, if a consumer purchases a second-hand device, the prior owner's 911 preferences should be easy for that consumer to edit or delete to fit his or her needs.

Auxiliary Data[11]

NG911 offers the opportunity to provide additional data to PSAPs and first responders, such as the caller's medical history, a description of the caller's residence or business location, and related data including building floor plans, information about hazardous materials, and building occupants with special needs. This data will often be maintained and provided by third parties such as health care organizations that maintain electronic records or commercial landlords that maintain floor plans. Since this auxiliary data may be considered part of the 911 call record and therefore subject to public disclosure, is there a need to protect the privacy of this data differently than the remainder of the call information?

Any auxiliary data must be protected separately from traditional 911 call information and to the greatest extent possible. For more on this issue we refer the Commission to our discussion above surrounding primary versus secondary information protection.

---

[10] *See* NOI, *supra* note 1, para. 58.

[11] *See* NOI, *supra* note 1, para. 61.

Authentication

The Electronic Frontier Foundation addresses the privacy and free speech risks associated with mandating authentication. We support EFF's statements and refer the Commission to EFF's reply comments in this proceeding for a complete discussion.

Education

Paragraph #78: What role will public information campaigns play in the transition to NG911?

Effective information campaigns will be integral to consumer education as NG911systems replace the outdated legacy 911 systems. Because NG911 focuses largely on improving emergency response through updating the 911system to support modern technology, consumers must be provided with high quality educational materials disseminated through multi-media channels. Information campaigns must also clearly lay out the capabilities of 911 systems so consumers do not attempt to call 911 through media that are not enabled by their particular system.

As an organization that provides educational materials to consumers, we also urge the Commission to encourage the appropriate entities to create easy-to-understand information campaigns that incorporate written, graphic, and auditory materials. Written materials should be made available at a 6th-grade reading level. Information in several languages is vitally important. When NG911 is launched, public service campaigns via broadcast and cable television should be deployed. And comprehensive information should be available via online resources.

IV. Concluding Remarks

The Privacy Rights Clearinghouse appreciates the opportunity to comment on NG911. An IP-based 911 system will provide consumers with more opportunity to communicate with 911 services and allow for improved response. With these benefits also come serious privacy challenges, however, and we strongly urge the Commission to take appropriate steps to protect consumer privacy.

Respectfully Submitted,

Beth Givens, Director
Meghan Bohn, Staff Attorney
Privacy Rights Clearinghouse
3100 5th Ave. Suite B
San Diego, CA 92103
www.privacyrights.org